

Frequently Asked Questions SIMM 5305-B and C – Plan of Action and Milestones

Q. Why are we being asked to do this? This seems to be more work without a purpose.

A. The purpose is to provide state entities with a tool and associated procedures to record and report deficiencies in a standardized way so that the California Information Security Office (CISO) may better track gaps and completion of remediation activities, and provide a means to better measure the State's overall risk. Where possible, the CISO may also be able to better assist the state entity with their challenges.

Q. The details you are asking for are minimal and not of sufficient detail for the CISO to manage the risks.

A. It is the responsibility of the state entity, not the CISO, to manage their risks. This simple tool is designed to collect the most basic of information and provide a statewide view of California's cyber security risks. This view will be enhanced when necessary by contacting the state entity. The data derived from the tool will also provide a means to assess state entity's prioritization of information security activities and their tasking individuals to address program gaps and areas of non-compliance in a timelier manner.

Q. Our department already has a plan on file with the CISO, but it is not in this format. Will those suffice until completed or do I need to resubmit using this new format?

A. All existing plans must be updated to the new format for consistency and data correlation and submitted to the CISO by November 2, 2015.

Q. Our department is already using an enterprise-wide system to collect this information and so much more. Can we simply submit a report generated by our system?

A. No. You must transfer information from your system to this tool. We kept the number of reporting cells to a minimum in order to limit impact. It is the goal of the CISO to implement a statewide system in the future that will provide all state entities a robust, web-based reporting, tracking, and managing capability. Until that is available, this simple reporting tool will be used.

Q. I'm still not sure exactly what I am to report on. Audit findings only?

A. The CISO requires state entities to submit a POAM for all security compliance deficiencies and significant Information Security risks that cannot be immediately addressed. These risks can be identified during numerous activities. Here are some examples:

- Your department hires a consulting firm to perform a comprehensive risk assessment of your entire organization (this is a top-to-bottom assessment, not simply a vulnerability scan and/or penetration test). The firm's final report lists a series of unmitigated vulnerabilities.
- Your department hires the California Department of the Military to perform a limited vulnerability scan of a selected subnet. They report finding 23 systems (clients and servers) that do not have the latest security patch installed and you will not be able to patch these system immediately. You will not report 23 deficiencies. Using the tool, you will report on 2 rows, 1 for the clients and 1 for the servers.
- Each year, your entity completes a Risk Management and Privacy Program Compliance Certification ([SIMM 5330-B](#)). Your entity is not able to certify 100% compliance to all sections of SAM and SIMM.
- You submit a Technology Recovery Plan to the CISO and receive feedback indicating an area where you are lacking minimum requirements.
- An information security incident occurs and you find that a control is missing that allowed the incident to occur. Your entity is not able to immediately "fix" that missing control.
- During the annual update and testing of your TRP, your entity discovers a critical step in recovering your mission critical computer systems is missing.
- Microsoft announces they will no longer support a specific server operating system after a future date and you have several such servers in production. Although that end-of-life (EOL) date has not arrived, your department will likely not retire the EOL system in time. Begin reporting this as a risk in the POAM report as soon as that determination is formulated.

Q. How often does the department need to provide progress updates?

A. Unless otherwise directed, progress updates must be submitted to the CISO every 90 days. Due to the nature of the information, submitters are to use the Secure File Transfer (SFT) system provided for this purpose.

Q. Do we submit a separate POAM for each risk, each SIMM certification, or each audit/assessment; or do you want a single consolidated POAM?

A. The latter. Reporting entities shall maintain only one master POAM that records all applicable security audit findings, compliance deficiencies, security risks, incident remediation activities, or other gaps in the entities' information security program. This master POAM must be kept updated at all times.

Q. Once we report a risk as “Completed” may we remove it?

A. When a reporting entity has submitted an updated master POAM where one or more risks reflect a status of “Completed” the CISO may request further information to support the “Completed” status. Once the CISO is satisfied, an acknowledgement will be sent to the reporting entity and the entity may then remove the risk from the POAM reporting tool.